



Utilizzare la API

StorageGRID 11.9

NetApp
November 08, 2024

Sommario

- Utilizzare la API 1
 - Utilizzare l'API Grid Management 1
 - Operazioni API di Grid Management 4
 - Versione dell'API Grid Management 5
 - Protezione contro la contraffazione delle richieste (CSRF) 7
 - Utilizzare l'API se è attivato il Single Sign-on 8
 - Disattivare le funzioni con l'API 21

Utilizzare la API

Utilizzare l'API Grid Management

È possibile eseguire attività di gestione del sistema utilizzando l'API REST di Grid Management invece dell'interfaccia utente di Grid Manager. Ad esempio, è possibile utilizzare l'API per automatizzare le operazioni o creare più entità, ad esempio gli utenti, più rapidamente.

Risorse di alto livello

L'API Grid Management fornisce le seguenti risorse di primo livello:

- `/grid`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate.
- `/org`: L'accesso è limitato agli utenti che appartengono a un gruppo LDAP locale o federato per un account tenant. Per ulteriori informazioni, vedere ["Utilizzare un account tenant"](#).
- `/private`: L'accesso è limitato agli utenti di Grid Manager e si basa sulle autorizzazioni di gruppo configurate. Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

Emettere richieste API

L'API Grid Management utilizza la piattaforma API open source Swagger. Swagger offre un'interfaccia utente intuitiva che consente a sviluppatori e non sviluppatori di eseguire operazioni in tempo reale in StorageGRID con l'API.

L'interfaccia utente di Swagger fornisce dettagli completi e documentazione per ogni operazione API.

Prima di iniziare

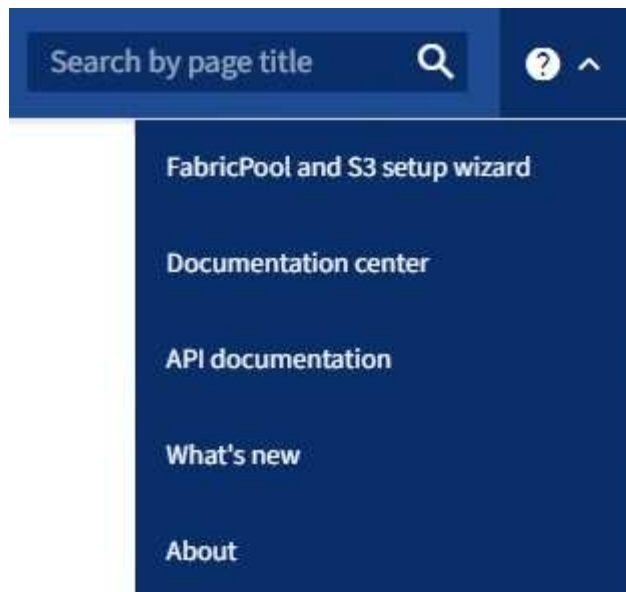
- L'utente ha effettuato l'accesso a Grid Manager utilizzando un ["browser web supportato"](#).
- Si dispone di ["autorizzazioni di accesso specifiche"](#).



Tutte le operazioni API eseguite utilizzando la pagina Web documentazione API sono operazioni in tempo reale. Fare attenzione a non creare, aggiornare o eliminare per errore i dati di configurazione o altri dati.

Fasi

1. Dall'intestazione Grid Manager, selezionare l'icona della guida e selezionare **documentazione API**.



2. Per eseguire un'operazione con l'API privata, selezionare **Vai alla documentazione API privata** nella pagina API di gestione StorageGRID.

Le API private sono soggette a modifiche senza preavviso. Gli endpoint privati di StorageGRID ignorano anche la versione API della richiesta.

3. Selezionare l'operazione desiderata.

Quando si espande un'operazione API, è possibile visualizzare le azioni HTTP disponibili, ad esempio GET, PUT, UPDATE ed DELETE.

4. Selezionare un'azione HTTP per visualizzare i dettagli della richiesta, tra cui l'URL dell'endpoint, un elenco di eventuali parametri obbligatori o facoltativi, un esempio del corpo della richiesta (se necessario) e le possibili risposte.

groups Operations on groups ▼

GET /grid/groups Lists Grid Administrator Groups 🔒

Parameters Try it out

Name	Description
type string <small>(query)</small>	filter by group type Available values : local, federated <input type="text" value="--"/>
limit integer <small>(query)</small>	maximum number of results Default value : 25 <input type="text" value="25"/>
marker string <small>(query)</small>	marker-style pagination offset (value is Group's URN) <input type="text" value="marker - marker-style pagination offset (value"/>
includeMarker boolean <small>(query)</small>	if set, the marker element is also returned <input type="text" value="--"/>
order string <small>(query)</small>	pagination order (desc requires marker) Available values : asc, desc <input type="text" value="--"/>

Responses Response content type

Code	Description
200	successfully retrieved Example Value Model <pre> { "responseTime": "2021-03-29T14:22:19.673Z", "status": "success", "apiVersion": "3.3", "deprecated": false, "data": [{ "displayName": "Developers", </pre>

5. Determinare se la richiesta richiede parametri aggiuntivi, ad esempio un ID utente o un gruppo. Quindi, ottenere questi valori. Potrebbe essere necessario emettere prima una richiesta API diversa per ottenere le informazioni necessarie.
6. Determinare se è necessario modificare il corpo della richiesta di esempio. In tal caso, è possibile selezionare **modello** per conoscere i requisiti di ciascun campo.
7. Selezionare **Provalo**.
8. Fornire i parametri richiesti o modificare il corpo della richiesta secondo necessità.
9. Selezionare **Esegui**.
10. Esaminare il codice di risposta per determinare se la richiesta ha avuto esito positivo.

Operazioni API di Grid Management

L'API Grid Management organizza le operazioni disponibili nelle seguenti sezioni.



Questo elenco include solo le operazioni disponibili nell'API pubblica.

- **Account:** Operazioni per la gestione degli account del tenant di storage, inclusa la creazione di nuovi account e il recupero dell'utilizzo dello storage per un determinato account.
- **Alert-history:** Operazioni su avvisi risolti.
- **Ricevitori di avvisi:** Operazioni sui destinatari di notifiche di avvisi (e-mail).
- **Alert-rules:** Operazioni sulle regole di allerta.
- **Silenzi di allerta:** Operazioni di silenzi di allerta.
- **Alerts:** Operazioni sugli avvisi.
- **Audit:** Operazioni per elencare e aggiornare la configurazione dell'audit.
- **Auth:** Operazioni per l'autenticazione della sessione utente.

L'API Grid Management supporta lo schema di autenticazione del token del bearer. Per accedere, è necessario fornire un nome utente e una password nel corpo JSON della richiesta di autenticazione (ovvero, `POST /api/v3/authorize`). Se l'utente viene autenticato correttamente, viene restituito un token di sicurezza. Questo token deve essere fornito nell'intestazione delle richieste API successive ("Authorization: Bearer *token*"). Il token scade dopo 16 ore.



Se per il sistema StorageGRID è attivato il single sign-on, è necessario eseguire diversi passaggi per l'autenticazione. Vedere "autenticazione nell'API se è attivato il single sign-on".

Per informazioni sul miglioramento della protezione dell'autenticazione, vedere "protezione contro la contraffazione delle richieste tra siti".

- **Certificati-client:** Operazioni per configurare i certificati client in modo che sia possibile accedere in modo sicuro a StorageGRID utilizzando strumenti di monitoraggio esterni.
- **Config:** Operazioni relative alla release del prodotto e alle versioni dell'API Grid Management. È possibile elencare la versione del prodotto e le principali versioni dell'API Grid Management supportate da tale release ed è possibile disattivare le versioni obsolete dell'API.
- **Disattivato-funzioni:** Operazioni per visualizzare le funzioni che potrebbero essere state disattivate.
- **dns-servers:** Operazioni per elencare e modificare i server DNS esterni configurati.
- **Dettagli unità:** Operazioni su unità per modelli di appliance di archiviazione specifici.
- **Nomi-dominio-endpoint:** Operazioni per elencare e modificare i nomi di dominio degli endpoint S3.
- **Erasure coding:** Operazioni sui profili di erasure coding.
- **Espansione:** Operazioni di espansione (a livello di procedura).
- **Expansion-node:** Operazioni di espansione (a livello di nodo).
- **Expansion-sites:** Operazioni di espansione (a livello di sito).
- **Grid-networks:** Operazioni per elencare e modificare l'elenco Grid Network.
- **Grid-password:** Operazioni per la gestione delle password grid.
- **Gruppi:** Operazioni per gestire i gruppi di amministratori di griglia locali e recuperare i gruppi di

amministratori di griglia federati da un server LDAP esterno.

- **Identity-source:** Operazioni per configurare un'origine di identità esterna e sincronizzare manualmente le informazioni di utenti e gruppi federati.
- **ilm:** Operazioni sulla gestione del ciclo di vita delle informazioni (ILM).
- **Procedure in corso:** Recupera le procedure di manutenzione attualmente in corso.
- **Licenza:** Operazioni per recuperare e aggiornare la licenza StorageGRID.
- **Logs:** Operazioni per la raccolta e il download dei file di log.v
- **Metriche:** Operazioni su metriche StorageGRID, incluse query metriche istantanee in un singolo punto nel tempo e query metriche di intervallo in un intervallo di tempo. L'API Grid Management utilizza lo strumento di monitoraggio dei sistemi Prometheus come origine dei dati back-end. Per informazioni sulla creazione di query Prometheus, visitare il sito Web Prometheus.



Le metriche che includono *private* nei loro nomi sono destinate esclusivamente all'uso interno. Queste metriche sono soggette a modifiche senza preavviso tra le versioni di StorageGRID.

- **Node-details:** Operazioni sui dettagli del nodo.
- **Node-Health:** Operazioni sullo stato di salute del nodo.
- **Node-storage-state:** Operazioni sullo stato dello storage del nodo.
- **ntp-servers:** Operazioni per elencare o aggiornare server NTP (Network Time Protocol) esterni.
- **Objects:** Operazioni su oggetti e metadati di oggetti.
- **Recovery:** Operazioni per la procedura di recovery.
- **Recovery-package:** Operazioni per il download del Recovery Package.
- **Regioni:** Operazioni per visualizzare e creare regioni.
- **s3-Object-lock:** Operazioni sulle impostazioni generali di blocco oggetti S3.
- **Server-certificate:** Operazioni per visualizzare e aggiornare i certificati del server Grid Manager.
- **snmp:** Operazioni sulla configurazione SNMP corrente.
- **Filigrane-archiviazione:** Filigrane del nodo di archiviazione.
- **Classi di traffico:** Operazioni per le policy di classificazione del traffico.
- **Untrusted-client-network:** Operazioni sulla configurazione Untrusted Client Network.
- **Utenti:** Operazioni per visualizzare e gestire gli utenti di Grid Manager.

Versione dell'API Grid Management

L'API Grid Management utilizza il controllo delle versioni per supportare aggiornamenti senza interruzioni.

Ad esempio, questo URL di richiesta specifica la versione 4 dell'API.

```
https://hostname_or_ip_address/api/v4/authorize
```

La versione principale dell'API viene modificata quando vengono apportate modifiche che sono *non compatibili* con le versioni precedenti. La versione secondaria dell'API viene modificata quando vengono apportate modifiche che sono *compatibili* con le versioni precedenti. Le modifiche compatibili includono l'aggiunta di

nuovi endpoint o di nuove proprietà.

Nell'esempio seguente viene illustrato il modo in cui la versione dell'API viene modificata in base al tipo di modifiche apportate.

Tipo di modifica all'API	Versione precedente	Nuova versione
Compatibile con le versioni precedenti	2,1	2,2
Non compatibile con versioni precedenti	2,1	3,0

Quando si installa il software StorageGRID per la prima volta, viene attivata solo la versione più recente dell'API. Tuttavia, quando si esegue l'aggiornamento a una nuova release di funzionalità di StorageGRID, si continua ad avere accesso alla versione precedente dell'API per almeno una release di funzionalità di StorageGRID.



È possibile configurare le versioni supportate. Per ulteriori informazioni, vedere la sezione **config** della documentazione Swagger API "[API di Grid Management](#)". È necessario disattivare il supporto per la versione precedente dopo aver aggiornato tutti i client API per utilizzare la versione più recente.

Le richieste obsolete vengono contrassegnate come obsolete nei seguenti modi:

- L'intestazione della risposta è "Deprecated: True"
- Il corpo di risposta JSON include "deprecato": Vero
- Viene aggiunto un avviso obsoleto a nms.log. Ad esempio:

```
Received call to deprecated v2 API at POST "/api/v2/authorize"
```

Determinare quali versioni API sono supportate nella release corrente

Utilizzare la `GET /versions` richiesta API per restituire un elenco delle versioni principali dell'API supportate. Questa richiesta si trova nella sezione **config** della documentazione dell'API Swagger.


```
GET https://{{IP-Address}}/api/versions
{
  "responseTime": "2023-06-27T22:13:50.750Z",
  "status": "success",
  "apiVersion": "4.0",
  "data": [
    2,
    3,
    4
  ]
}
```

Specificare una versione API per una richiesta

È possibile specificare la versione API utilizzando un parametro di percorso (`/api/v4`) o un'intestazione (`Api-Version: 4`). Se si forniscono entrambi i valori, il valore dell'intestazione sovrascrive il valore del percorso.

```
curl https://[IP-Address]/api/v4/grid/accounts

curl -H "Api-Version: 4" https://[IP-Address]/api/grid/accounts
```

Protezione contro la contraffazione delle richieste (CSRF)

Puoi contribuire a proteggere dagli attacchi di cross-site request forgery (CSRF) contro StorageGRID utilizzando i token CSRF per migliorare l'autenticazione che utilizza i cookie. Grid Manager e Tenant Manager abilitano automaticamente questa funzionalità di sicurezza; altri client API possono scegliere se attivarla al momento dell'accesso.

Un utente malintenzionato in grado di inviare una richiesta a un sito diverso (ad esempio con UN HTTP Form POST) può causare l'esecuzione di determinate richieste utilizzando i cookie dell'utente che ha effettuato l'accesso.

StorageGRID aiuta a proteggere dagli attacchi CSRF utilizzando token CSRF. Se attivato, il contenuto di un cookie specifico deve corrispondere al contenuto di un'intestazione specifica o di un parametro POST-body specifico.

Per attivare la funzione, impostare il `csrfToken` parametro su `true` durante l'autenticazione. L'impostazione predefinita è `false`.

```
curl -X POST --header "Content-Type: application/json" --header "Accept: application/json" -d "{
  \"username\": \"MyUserName\",
  \"password\": \"MyPassword\",
  \"cookie\": true,
  \"csrfToken\": true
}" "https://example.com/api/v3/authorize"
```

Quando true, un `GridCsrfToken` cookie viene impostato con un valore casuale per i login al Grid Manager e il `AccountCsrfToken` cookie viene impostato con un valore casuale per i login al Tenant Manager.

Se il cookie è presente, tutte le richieste che possono modificare lo stato del sistema (POST, PUT, PATCH, DELETE) devono includere una delle seguenti opzioni:

- L'`X-Csrf-Token` intestazione, con il valore dell'intestazione impostato sul valore del cookie del token CSRF.
- Per gli endpoint che accettano un corpo codificato in forma: Un `csrfToken` parametro del corpo della richiesta codificato in forma.

Per ulteriori esempi e dettagli, consultare la documentazione API online.



Le richieste che dispongono di un set di cookie token CSRF applicheranno anche l'intestazione "Content-Type: Application/json" per qualsiasi richiesta che prevede un corpo di richiesta JSON come protezione aggiuntiva contro gli attacchi CSRF.

Utilizzare l'API se è attivato il Single Sign-on

Utilizzare l'API se è attivato il single sign-on (Active Directory)

Se "[SSO \(Single Sign-on\) configurato e abilitato](#)" si utilizza Active Directory come provider SSO, è necessario eseguire una serie di richieste API per ottenere un token di autenticazione valido per l'API di gestione griglia o l'API di gestione tenant.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO.

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Lo `storagegrid-ssoauth.py` script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` per Red Hat Enterprise Linux, `./debs per Ubuntu o Debian e `./vsphere per VMware).`

- Un esempio di workflow di richieste di curl.

Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: A valid SubjectConfirmation was not found on this Response.



L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: Unsupported SAML version.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare `storagegrid-ssoauth.py` lo script Python. Andare alla fase 2.
 - USA richieste di curl. Andare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` lo script, passare lo script all'interprete Python ed eseguire lo script.

Quando richiesto, inserire i valori per i seguenti argomenti:

- Il metodo SSO. Immettere ADFS o adfs.
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID
- L'indirizzo per StorageGRID
- L'ID account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: adfs
saml_user: my-sso-username
saml_domain: my-domain
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'  
export SAMLPASSWORD='my-password'  
export SAMLDOMAIN='my-domain'  
export TENANTACCOUNTID='12345'  
export STORAGEGRID_ADDRESS='storagegrid.example.com'  
export AD_FS_ADDRESS='adfs.example.com'
```



Per accedere all'API Grid Management, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a `/api/v3/authorize-saml` e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a `python -m json.tool` per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \  
  -H "accept: application/json" -H "Content-Type: application/json" \  
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m \  
  json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{  
  "apiVersion": "3.0",  
  "data":  
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZHLbsIwEEV%2FJTuv7...  
  sS1%2BfQ33cvfwA%3D&RelayState=12345",  
  "responseTime": "2018-11-06T16:30:23.355Z",  
  "status": "success"  
}
```

- c. Salvare `SAMLRequest` dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST='fZHLbsIwEEV%2FJTuv7...sS1%2BfQ33cvfwA%3D'
```

- d. Ottenere un URL completo che includa l'ID della richiesta del client da ad FS.

Un'opzione consiste nel richiedere il modulo di accesso utilizzando l'URL della risposta precedente.

```
curl "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID" | grep 'form method="post" id="loginForm"'
```

La risposta include l'ID della richiesta del client:

```
<form method="post" id="loginForm" autocomplete="off" novalidate="novalidate" onKeyPress="if (event && event.keyCode == 13) Login.submitLoginRequest();" action="/adfs/ls/?SAMLRequest=fZHRTomwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de" >
```

e. Salvare l'ID della richiesta del client dalla risposta.

```
export SAMLREQUESTID='00000000-0000-0000-ee02-0080000000de'
```

f. Inviare le credenziali all'azione del modulo della risposta precedente.

```
curl -X POST "https://$AD_FS_ADDRESS/adfs/ls/?SAMLRequest=$SAMLREQUEST&RelayState=$TENANTACCOUNTID&client-request-id=$SAMLREQUESTID" \ --data "UserName=$SAMLUSER@$SAMLDOMAIN&Password=$SAMPLPASSWORD&AuthMethod=FormsAuthentication" --include
```

AD FS restituisce un reindirizzamento 302, con informazioni aggiuntive nelle intestazioni.



Se l'autenticazione a più fattori (MFA) è attivata per il sistema SSO, il post del modulo conterrà anche la seconda password o altre credenziali.

```
HTTP/1.1 302 Found
Content-Length: 0
Content-Type: text/html; charset=utf-8
Location:
https://adfs.example.com/adfs/ls/?SAMLRequest=fZHRTomwFIZfhb...UJikvo77sXPw%3D%3D&RelayState=12345&client-request-id=00000000-0000-0000-ee02-0080000000de
Set-Cookie: MSISAuth=AAEAADAvsHpXk6ApV...pmP0aEiNtJvWY=; path=/adfs; HttpOnly; Secure
Date: Tue, 06 Nov 2018 16:55:05 GMT
```

g. Salvare il MSISAuth cookie dalla risposta.

- j. Utilizzando il salvato `SAMLResponse`, eseguire una richiesta `StorageGRID/api/saml-response` per generare un token di autenticazione `StorageGRID`.

Per `RelayState`, utilizzare l'ID `account tenant` o `0` se si desidera accedere all'API di gestione griglia.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \  
-H "accept: application/json" \  
--data-urlencode "SAMLResponse=$SAMLResponse" \  
--data-urlencode "RelayState=$TENANTACCOUNTID" \  
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{  
  "apiVersion": "3.0",  
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",  
  "responseTime": "2018-11-07T21:32:53.486Z",  
  "status": "success"  
}
```

- a. Salvare il token di autenticazione nella risposta come `MYTOKEN`.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

È ora possibile utilizzare `MYTOKEN` per altre richieste, in modo simile a come si userebbe l'API se non fosse utilizzato SSO.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza Active Directory come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API `StorageGRID` disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da `StorageGRID`, che richiede un token bearer `StorageGRID` valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--cookie "sso=true" \  
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{  
  "apiVersion": "3.0",  
  "data":  
  "https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",  
  "responseTime": "2018-11-20T22:20:30.839Z",  
  "status": "success"  
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST  
='https://adfs.example.com/adfs/ls/?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found  
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256  
Set-Cookie: MSISignoutProtocol=U2FtbA==; expires=Tue, 20 Nov 2018 22:35:03 GMT; path=/adfs; HttpOnly; Secure
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.


```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--include
```

Una 204 No Content risposta indica che l'utente è stato disconnesso.

```
HTTP/1.1 204 No Content
```

Utilizzare l'API se è attivato il single sign-on (Azure)

Se "[SSO \(Single Sign-on\) configurato e abilitato](#)" si utilizza Azure come provider SSO, è possibile utilizzare due script di esempio per ottenere un token di autenticazione valido per l'API di gestione griglia o l'API di gestione tenant.

Accedere all'API se Azure Single Sign-on è attivato

Queste istruzioni sono valide se si utilizza Azure come provider di identità SSO

Prima di iniziare

- Si conoscono l'indirizzo e-mail SSO e la password di un utente federato che appartiene a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare i seguenti script di esempio:

- `storagegrid-ssoauth-azure.py` Lo script Python
- `storagegrid-ssoauth-azure.js` script Node.js

Entrambi gli script si trovano nella directory dei file di installazione di StorageGRID (`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian e `./vsphere` per VMware).

Per scrivere la tua integrazione dell'API con Azure, consulta `storagegrid-ssoauth-azure.py` lo script. Lo script Python effettua due richieste direttamente a StorageGRID (prima per ottenere la SAMLRequest e poi per ottenere il token di autorizzazione) e chiama anche lo script Node.js per interagire con Azure per eseguire le operazioni SSO.

Le operazioni SSO possono essere eseguite utilizzando una serie di richieste API, ma non è semplice. Il modulo Puppeteer Node.js viene utilizzato per scrapare l'interfaccia SSO di Azure.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: `Unsupported SAML version`.

Fasi

1. Installare le dipendenze richieste, come indicato di seguito:

- a. Installare Node.js (vedere "<https://nodejs.org/en/download/>").
- b. Installare i moduli Node.js richiesti (puppeteer e jsdom):

```
npm install -g <module>
```

2. Passare lo script Python all'interprete Python per eseguirlo.

Lo script Python chiamerà quindi lo script Node.js corrispondente per eseguire le interazioni SSO di Azure.

3. Quando richiesto, immettere i valori per i seguenti argomenti (o passarli utilizzando i parametri):
 - Indirizzo e-mail SSO utilizzato per accedere ad Azure
 - L'indirizzo per StorageGRID
 - L'ID account tenant, se si desidera accedere all'API di gestione tenant
4. Quando richiesto, inserire la password e prepararsi a fornire un'autorizzazione MFA ad Azure, se richiesto.

```
c:\Users\user\Documents\azure_sso>py storagegrid-azure-ssoauth.py --sso-email-address user@my-domain.com
--sg-address storagegrid.examp.e.com --tenant-account-id 0
Enter the user's SSO password:
*****

Watch for and approve a 2FA authorization request
*****
StorageGRID Auth Token: {'responseTime': '2021-10-04T21:30:48.807Z', 'status': 'success', 'apiVersion':
'3.4', 'data': '4807d93e-a3df-48f2-9680-906cd255979e'}
```



Lo script presuppone che l'autenticazione MFA venga eseguita utilizzando Microsoft Authenticator. Potrebbe essere necessario modificare lo script per supportare altre forme di MFA (ad esempio l'immissione di un codice ricevuto in un messaggio di testo).

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

Utilizzare l'API se è attivato il Single Sign-on (PingFederate)

Se "[SSO \(Single Sign-on\) configurato e abilitato](#)" si utilizza PingFederate come provider SSO, è necessario emettere una serie di richieste API per ottenere un token di autenticazione valido per l'API di gestione griglia o l'API di gestione tenant.

Accedere all'API se è attivato il Single Sign-on

Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

Prima di iniziare

- Si conoscono il nome utente e la password SSO di un utente federated appartenente a un gruppo di utenti StorageGRID.
- Se si desidera accedere all'API di gestione tenant, si conosce l'ID account tenant.

A proposito di questa attività

Per ottenere un token di autenticazione, è possibile utilizzare uno dei seguenti esempi:

- Lo `storagegrid-ssoauth.py` script Python, che si trova nella directory dei file di installazione di StorageGRID (`./rpms` per Red Hat Enterprise Linux, `./debs` per Ubuntu o Debian e

./vsphere per VMware).

- Un esempio di workflow di richieste di curl.

Il flusso di lavoro di arricciatura potrebbe andare in timeout se viene eseguito troppo lentamente. Potrebbe essere visualizzato l'errore: A valid SubjectConfirmation was not found on this Response.



L'esempio di workflow di curl non protegge la password da essere vista da altri utenti.

Se si verifica un problema di codifica URL, potrebbe essere visualizzato l'errore: Unsupported SAML version.

Fasi

1. Selezionare uno dei seguenti metodi per ottenere un token di autenticazione:
 - Utilizzare `storagegrid-ssoauth.py` lo script Python. Andare alla fase 2.
 - USA richieste di curl. Andare alla fase 3.
2. Se si desidera utilizzare `storagegrid-ssoauth.py` lo script, passare lo script all'interprete Python ed eseguire lo script.

Quando richiesto, inserire i valori per i seguenti argomenti:

- Il metodo SSO. È possibile inserire qualsiasi variazione di "pingfederate" (PINGFEDERATE, pingfederate e così via).
- Il nome utente SSO
- Il dominio in cui è installato StorageGRID. Questo campo non viene utilizzato per PingFederate. È possibile lasciare vuoto il campo o inserire un valore qualsiasi.
- L'indirizzo per StorageGRID
- L'ID account tenant, se si desidera accedere all'API di gestione tenant.

```
python3 storagegrid-ssoauth.py
sso_method: pingfederate
saml_user: my-sso-username
saml_domain:
sg_address: storagegrid.example.com
tenant_account_id: 12345
Enter the user's SAML password:
*****
*****
StorageGRID Auth Token: 56eb07bf-21f6-40b7-afob-5c6cacfb25e7
```

Il token di autorizzazione StorageGRID viene fornito nell'output. È ora possibile utilizzare il token per altre richieste, in modo simile a come si utilizzerebbe l'API se SSO non fosse utilizzato.

3. Se si desidera utilizzare le richieste di arricciamento, attenersi alla seguente procedura.
 - a. Dichiarare le variabili necessarie per l'accesso.

```
export SAMLUSER='my-sso-username'  
export SAMLPASSWORD='my-password'  
export TENANTACCOUNTID='12345'  
export STORAGEGRID_ADDRESS='storagegrid.example.com'
```



Per accedere all'API Grid Management, utilizzare 0 come TENANTACCOUNTID.

- b. Per ricevere un URL di autenticazione firmato, inviare una richiesta POST a `/api/v3/authorize-saml` e rimuovere la codifica JSON aggiuntiva dalla risposta.

Questo esempio mostra una richiesta POST per un URL di autenticazione firmato per TENANTACCOUNTID. I risultati verranno passati a `python -m json.tool` per rimuovere la codifica JSON.

```
curl -X POST "https://$STORAGEGRID_ADDRESS/api/v3/authorize-saml" \  
  -H "accept: application/json" -H "Content-Type: application/json" \  
  --data "{\"accountId\": \"$TENANTACCOUNTID\"}" | python -m \  
  json.tool
```

La risposta per questo esempio include un URL firmato con codifica URL, ma non include il layer di codifica JSON aggiuntivo.

```
{  
  "apiVersion": "3.0",  
  "data": "https://my-pf-baseurl/idp/SSO.saml2?...",  
  "responseTime": "2018-11-06T16:30:23.355Z",  
  "status": "success"  
}
```

- c. Salvare SAMLRequest dalla risposta per l'utilizzo nei comandi successivi.

```
export SAMLREQUEST="https://my-pf-baseurl/idp/SSO.saml2?..."
```

- d. Esportare la risposta e il cookie e visualizzare la risposta:

```
RESPONSE=$(curl -c - "$SAMLREQUEST")
```

```
echo "$RESPONSE" | grep 'input type="hidden" name="pf.adapterId"  
id="pf.adapterId"'
```

e. Esportare il valore 'pf.adapterId' e visualizzare la risposta:

```
export ADAPTER='myAdapter'
```

```
echo "$RESPONSE" | grep 'base'
```

f. Esportare il valore 'href' (rimuovere la barra finale /) e visualizzare la risposta:

```
export BASEURL='https://my-pf-baseurl'
```

```
echo "$RESPONSE" | grep 'form method="POST"'
```

g. Esportare il valore "azione":

```
export SSOPING='/idp/.../resumeSAML20/idp/SSO.ping'
```

h. Invia cookie con credenziali:

```
curl -b <(echo "$RESPONSE") -X POST "$BASEURL$SSOPING" \  
--data "pf.username=$SAMLUSER&pf.pass=  
$SAMLPASSWORD&pf.ok=clicked&pf.cancel=&pf.adapterId=$ADAPTER" \  
--include
```

i. Salvare il SAMLResponse dal campo nascosto:

```
export SAMLResponse='PHNhbWxwOlJlc3BvbnN...1scDpSZXNwb25zZT4='
```

j. Utilizzando il salvato SAMLResponse, eseguire una richiesta StorageGRID/api/saml-response per generare un token di autenticazione StorageGRID.

Per RelayState, utilizzare l'ID account tenant o 0 se si desidera accedere all'API di gestione griglia.

```
curl -X POST "https://$STORAGEGRID_ADDRESS:443/api/saml-response" \  
-H "accept: application/json" \  
--data-urlencode "SAMLResponse=$SAMLResponse" \  
--data-urlencode "RelayState=$TENANTACCOUNTID" \  
| python -m json.tool
```

La risposta include il token di autenticazione.

```
{
  "apiVersion": "3.0",
  "data": "56eb07bf-21f6-40b7-af0b-5c6cacfb25e7",
  "responseTime": "2018-11-07T21:32:53.486Z",
  "status": "success"
}
```

a. Salvare il token di autenticazione nella risposta come MYTOKEN.

```
export MYTOKEN="56eb07bf-21f6-40b7-af0b-5c6cacfb25e7"
```

È ora possibile utilizzare MYTOKEN per altre richieste, in modo simile a come si userebbe l'API se non fosse utilizzato SSO.

Disconnettersi dall'API se è attivato il Single Sign-on

Se è stato attivato il Single Sign-on (SSO), è necessario emettere una serie di richieste API per disconnettersi dall'API Grid Management o dall'API Tenant Management. Queste istruzioni sono valide se si utilizza PingFederate come provider di identità SSO

A proposito di questa attività

Se necessario, è possibile disconnettersi dall'API StorageGRID disconnettendosi dalla singola pagina di disconnessione dell'organizzazione. In alternativa, è possibile attivare il logout singolo (SLO) da StorageGRID, che richiede un token bearer StorageGRID valido.

Fasi

1. Per generare una richiesta di disconnessione firmata, passare `cookie "sso=true" all'API SLO:

```
curl -k -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \
-H "accept: application/json" \
-H "Authorization: Bearer $MYTOKEN" \
--cookie "sso=true" \
| python -m json.tool
```

Viene restituito un URL di disconnessione:

```
{
  "apiVersion": "3.0",
  "data": "https://my-ping-
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D",
  "responseTime": "2021-10-12T22:20:30.839Z",
  "status": "success"
}
```

2. Salvare l'URL di disconnessione.

```
export LOGOUT_REQUEST='https://my-ping-  
url/idp/SLO.saml2?SAMLRequest=fZDNboMwEIRfhZ...HcQ%3D%3D'
```

3. Inviare una richiesta all'URL di disconnessione per attivare SLO e reindirizzare a StorageGRID.

```
curl --include "$LOGOUT_REQUEST"
```

Viene restituita la risposta 302. La posizione di reindirizzamento non è applicabile alla disconnessione API-only.

```
HTTP/1.1 302 Found  
Location: https://$STORAGEGRID_ADDRESS:443/api/saml-  
logout?SAMLResponse=fVLLasMwEPwVo7ss%...%23rsa-sha256  
Set-Cookie: PF=QoKs...SgCC; Path=/; Secure; HttpOnly; SameSite=None
```

4. Eliminare il token del bearer StorageGRID.

L'eliminazione del token portante StorageGRID funziona come senza SSO. Se `cookie "sso=true" non viene fornito, l'utente viene disconnesso da StorageGRID senza influire sullo stato SSO.

```
curl -X DELETE "https://$STORAGEGRID_ADDRESS/api/v3/authorize" \  
-H "accept: application/json" \  
-H "Authorization: Bearer $MYTOKEN" \  
--include
```

Una 204 No Content risposta indica che l'utente è stato disconnesso.

```
HTTP/1.1 204 No Content
```

Disattivare le funzioni con l'API

È possibile utilizzare l'API di gestione griglia per disattivare completamente alcune funzionalità nel sistema StorageGRID. Quando una funzione viene disattivata, non è possibile assegnare a nessuno le autorizzazioni per eseguire le attività correlate a tale funzione.

A proposito di questa attività

Il sistema Disattivato consente di impedire l'accesso a determinate funzioni del sistema StorageGRID. La disattivazione di una funzione è l'unico modo per impedire all'utente root o agli utenti appartenenti a gruppi di amministratori con autorizzazione **Root Access** di utilizzare tale funzione.

Per comprendere come questa funzionalità potrebbe essere utile, considerare il seguente scenario:

L'azienda A è un provider di servizi che affitta la capacità di storage del proprio sistema StorageGRID creando account tenant. Per proteggere la sicurezza degli oggetti dei titolari di leasing, la Società A desidera garantire che i propri dipendenti non possano mai accedere a alcun account tenant dopo l'implementazione dell'account.

*L'azienda A è in grado di raggiungere questo obiettivo utilizzando il sistema Deactivate Features nell'API Grid Management. Disattivando completamente la funzione **Cambia password root tenant** in Grid Manager (sia l'interfaccia utente che l'API), l'azienda A garantisce che gli utenti Admin, inclusi l'utente root e gli utenti appartenenti a gruppi con autorizzazione **root access**, non possano modificare la password per l'utente root di qualsiasi account tenant.*

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia. Vedere "[Utilizzare l'API Grid Management](#)".
2. Individuare l'endpoint Deactivate Features.
3. Per disattivare una funzione, ad esempio Modifica password root tenant, inviare un corpo all'API come segue:

```
{ "grid": {"changeTenantRootPassword": true} }
```

Al termine della richiesta, la funzione Modifica password root tenant viene disattivata. L'autorizzazione di gestione **Modifica password principale tenant** non viene più visualizzata nell'interfaccia utente e qualsiasi richiesta API che tenti di modificare la password principale per un tenant non riesce con "403 Proibito".

Riattivare le funzioni disattivate

Per impostazione predefinita, è possibile utilizzare l'API Grid Management per riattivare una funzione disattivata. Tuttavia, se si desidera evitare che le funzioni disattivate vengano riattivate, è possibile disattivare la funzione **ActivateFeatures**.



Impossibile riattivare la funzione **ActivateCaratures**. Se decidi di disattivare questa funzione, tieni presente che perderai in modo permanente la possibilità di riattivare qualsiasi altra funzione disattivata. È necessario contattare il supporto tecnico per ripristinare eventuali funzionalità perse.

Fasi

1. Accedere alla documentazione Swagger per l'API di gestione griglia.
2. Individuare l'endpoint Deactivate Features.
3. Per riattivare tutte le funzioni, inviare un corpo all'API come segue:

```
{ "grid": null }
```

Una volta completata la richiesta, tutte le funzioni, inclusa la funzione Change tenant root password, vengono riattivate. L'autorizzazione di gestione **Change tenant root password** viene ora visualizzata nell'interfaccia utente e tutte le richieste API che tentano di modificare la password root per un tenant avranno esito positivo, presupponendo che l'utente disponga dell'autorizzazione di gestione **Root access** o **Change tenant root password**.



L'esempio precedente causa la riattivazione di *tutte* le funzioni disattivate. Se sono state disattivate altre funzioni che devono rimanere disattivate, è necessario specificarle esplicitamente nella richiesta PUT. Ad esempio, per riattivare la funzione Cambia password root tenant e continuare a disattivare l'autorizzazione di gestione storageAdmin, inviare la richiesta PUT:

```
{ "grid": {"storageAdmin": true} }
```

Informazioni sul copyright

Copyright © 2024 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.